UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

PAMELA BUMP, MELISSA CHARBONNEAU, DOUGLAS CONLEY, NOAH HELVEY, DALLIN ILER, DUSTIN JONES, DEVINNE PETERSON, JUSTIN RANDALL, SOFIA RODRIGUEZ, and RACHEL WOODS, individually and on behalf of all others similarly situated, Plaintiffs, v. NELNET SERVICING, LLC Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Pamela Bump, Melissa Charbonneau, Douglas Conley, Noah Helvey, Dallin Iler, Dustin Jones, Devinne Peterson, Justin Randall, Sofia Rodriguez, and Rachel Woods ("Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendant Nelnet Servicing, LLC ("Nelnet" or "Defendant") based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Plaintiffs bring this class action against Nelnet for its (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information, including without limitation, names, addresses, email addresses, phone numbers, and Social Security numbers (collectively "PII"); (ii) failure to comply with industry standards to protect information systems that contain PII; (iii) unlawful disclosure of Plaintiffs' and Class Members' PII; and (iv) failure to provide adequate notice to Plaintiffs and other Class Members that their PII had been disclosed and compromised.

2. Nelnet is one of the largest student loan servicers in the United States, servicing $589 billion in student loans for over 17 million borrowers.

3. In addition to servicing student loans, Nelnet provides online technology services such as web portal and payment processing services to other student loan servicers, including EdFinancial and the Oklahoma Student Loan Authority ("OSLA").

4. On August 26, 2022, Nelnet began publicly notifying state Attorneys General and 2,501,324 impacted current and former Nelnet account holders that the PII of the 2,501,324 impacted individuals had been accessed and stolen by an unauthorized third-party (the "Data Breach").

5. By August 26, 2022, Nelnet had known of the data breach for over a month but had failed to notify a single impacted individual. Nelnet chose to notify individuals via U.S Mail in letters entitled "Notice of Security Incident."

6. As a result of Nelnet's failures and lax security protocols, hackers gained access to Nelnet's computer systems and/or servers and were able to steal the personal information of millions of customers, including their Social Security numbers, phone numbers, emails, and addresses (the "Data Breach").

7. The Data Breach was a direct and proximate result of Nelnet's flawed online system configuration and design and Nelnet's failure to implement and follow basic security procedures.

8. Because of Nelnet's failures, unauthorized individuals were able to access and pilfer Plaintiffs' and Class Members' PII.

9. As a result, Plaintiffs and Class Members are at substantially increased risk of future identity theft, both currently and for the indefinite future. Plaintiffs' and Class Members'

PII, including their Social Security numbers, that were compromised by cyber criminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft.

10. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, breach of confidence, invasion of privacy—intrusion upon seclusion, violations of consumer protection statutes of their home states, violations of data protection statutes of their home states, and injunctive relief claims.

11. Plaintiffs seek damages and injunctive relief requiring Nelnet to adopt reasonably sufficient practices to safeguard the PII that remains in Nelnet's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

12. Given that information relating to the Data Breach, including the systems that were impacted, the configuration and design of Defendant's website and systems remain exclusively in Defendant's control, Plaintiffs anticipate additional support for their claims will be uncovered following a reasonable opportunity for discovery.

JURISDICTION AND VENUE

13. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class and Subclass exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative Members of the Class and Subclass defined below, and a significant portion of putative Class and Subclass Members are citizens of a different state than Defendant.

14. This Court has personal jurisdiction over Defendant Nelnet because Defendant Nelnet is a resident of the State of Nebraska.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Nelnet resides in this District.

16. Plaintiffs' claims arise out of or relate to Nelnet's contacts with California. Nelnet has intentionally created extensive contacts with California through its deliberate marketing and sale of its services in the forum.

PARTIES

17. Plaintiff Pamela Bump ("Plaintiff Bump") is a citizen and resident of the Commonwealth of Massachusetts.

18. Plaintiff Melissa Charbonneau ("Plaintiff Charbonneau") is a citizen and resident of the State of Illinois.

19. Plaintiff Douglas Conley ("Plaintiff Conley") is a citizen and resident of the State of Arizona.

20. Plaintiff Noah Helvey ("Plaintiff Helvey") is a citizen and resident of the State of Utah.

21. Plaintiff Dallin Iler ("Plaintiff Iler") is a citizen and resident of the State of Indiana.

22. Plaintiff Dustin Jones ("Plaintiff Jones") is a citizen and resident of the Commonwealth of Pennsylvania.

23. Plaintiff Devinne Peterson ("Plaintiff Peterson") is a citizen and resident of the Commonwealth of Pennsylvania.

24. Plaintiff Justin Randall ("Plaintiff Randall") is a citizen and resident of the State of Wisconsin.

25. Plaintiff Sofia Rodriguez ("Plaintiff Rodriguez") is a citizen and resident of the State of Michigan.

26. Plaintiff Rachel Woods ("Plaintiff Woods") is a citizen and resident of the State of Texas.

27. Defendant Nelnet Servicing, LLC ("Nelnet") is Nebraska limited liability company with its principal place of business located at 121 South 13th Street, Suite 100, Lincoln, Nebraska, 68508.

FACTUAL BACKGROUND

I. Defendant Nelnet Servicing, LLC

28. Nelnet is a Nebraska-based company which primarily "engage[s] in student loan servicing, tuition payment processing and school information systems, and communications" and primarily makes money via "net interest income earned on a portfolio of federally insured student loans."[1] In other words, Nelnet primarily serves as a student loan servicer for individuals that have taken out federal student loans and makes money via the interest it charges individuals on their student loan balances. As of June 30, 2022, the Nelnet was servicing $589.5 billion in loans for 17.4 million borrowers.[2]

29. Nelnet also earns revenue providing technology services such as website portal and payment processing to other student loan and debt servicers, [3] such EdFinancial and the Oklahoma Student Loan Authority ("OSLA").

[1] *About Us*, NELNET, https://www.nelnetinvestors.com/Home/default.aspx (accessed Sept. 6, 2022).
[2] *Nelnet 10Q Earnings Release*, NELNET (Aug. 8, 2022) https://s21.q4cdn.com/368920761/files/doc_financials/2022/q2/8K-Exhibit-99.1-8.8.22-10Q-Earnings-Release-FINAL.pdf (accessed Sept. 6, 2022).
[3] *Id.*

30. No individual voluntarily engages Nelnet as their student loan servicer or payment portal provider. Instead, Nelnet is given an individuals' federal loans to service without any choice or input given to the individual or is similarly chosen by a federal student loan servicer such as EdFinancial or OSLA to provide web portal and payment processing services without any input from the individual.

II. Nelnet Obtains, Collects, and Stores Account Holders' PII

31. Nelnet requires all individuals to provide their sensitive, personal, and private protected information to register and create an account with Nelnet to use Nelnet's services.

32. Thus, all individuals whose federal student loans are assigned (without their input) to Nelnet must register with Nelnet and provide their PII to Nelnet to track and make payments on their federal student loans. Similarly, individuals whose federal student loans are serviced by a loan servicer that engages Nelnet to provide web portal or payment processing services must register and create an account with Nelnet and provide their PII to Nelnet.

33. Nelnet maintains, keeps, and exploits customers' PII for Nelnet's own benefit, including long after individuals have paid off their loans in full and cease being Nelnet customers.

34. Nelnet is in complete operation, control, and supervision of its website and systems, and Nelnet intentionally configured and designed its website and systems this way in order to make more money without regard to Plaintiffs' and Class Members' PII.

35. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, Nelnet assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

36. Plaintiffs and Class Members reasonably expect that student loan service providers such as Nelnet will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

37. Nelnet acknowledges that it has an obligation to protect PII from disclosure and thus makes the following representation on the Nelnet website:

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.[4]

38. Despite the above representations, Nelnet failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

39. Had Nelnet followed industry guidelines and adopted reasonably security measures as represented in the Nelnet Privacy Policy, Nelnet would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

III. FTC Guidelines

40. Nelnet is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable

[4] *Nelnet Privacy Policy Mission Statement, Our Security Procedures*, NELNET, https://www.nelnet.com/privacy-and-security#:~:text=As%20stated%20above%20we%20do,Comply%20with%20the%20law (accessed Sept 6, 2022).

and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

41. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

42. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

43. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

45. Nelnet failed to properly implement basic data security practices. Nelnet's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals, as reflected by

the sensitive Social Security information stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

46. Nelnet was always fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. Nelnet was also aware of the significant repercussions that would result from its failure to do so.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach

47. Beginning in June 2022, Nelnet allowed an unauthorized third-party to access Plaintiffs' and Class Members' student loan account registration information, including their names, addresses, email addresses, phone numbers, and Social Security numbers. According to Nelnet, this unauthorized access continued through July 22, 2022.

48. Nelnet did not discover the unauthorized access until July 21, 2022, when Nelnet claims to have notified EdFinancial and OSLA about the vulnerability and unauthorized access.

49. Despite discovering the Data Breach July 21, 2022, Nelnet did not notify the U.S. Department of Education of the Data Breach until after August 17, 2022 and did not begin notifying impacted customers until August 26, 2022.

II. Nelnet's Data Security Failures Caused the Data Breach

50. Up to, and including, the period when the Data Breach occurred, Nelnet breached its duties, obligations, and promises to Plaintiffs and Class Members, by its failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

c. address well-known warnings that its systems and servers were susceptible to a data breach;

d. implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its systems that accessed customers' personal information and otherwise would have protected customers' sensitive personal information;

e. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented customers' sensitive personal information from being stolen. Specifically, there are recommended, available measures to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems; and

f. adequately safeguard customers' sensitive personal information and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

III. Nelnet's Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

51. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

54. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations.

55. Prior to the Data Breach, and during the breach itself, Nelnet failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security.

Furthermore, by failing to have reasonable data security measures in place, Nelnet engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

IV. The Value of the Disclosed PII and Effects of Unauthorized Disclosure

56. Nelnet understood the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

57. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

58. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

59. The forms of PII involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with

those entities.

60. Indeed, even the Social Security Administration (‘‘SSA”) warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

61. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

62. The ramifications of Defendants’ failure to keep Plaintiffs’ and Class Members’ PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the “dark web” may take months or more to reach end-users, in part because the data is often sold in small batches as

opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

63. Thus, Nelnet knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Nelnet failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

64. As highly sophisticated parties that handle sensitive PII, Nelnet failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

65. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

66. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

67. There is often a lag time between when fraud occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

68. Personal is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

69. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

70. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

V. The Data Breach Damaged Plaintiffs and Class Members.

71. As a result of Nelnet's deficient security measures, Plaintiffs and Class Members have been harmed by the compromise of their sensitive personal information, which is likely currently for sale on the dark web and through private sale to other cyber criminals and/or being used by criminals for identify theft and other fraud-related crimes.

72. Plaintiffs and Class Members face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their Social Security numbers, emails, phone numbers, and physical addresses as a result of the breach. These specific types of information are associated with a high risk of fraud.

73. Criminals have fraudulently applied for credit cards using the PII of Plaintiffs and Class Member such as Plaintiff Jones.

74. Many Class Members will also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

75. Plaintiffs and Class Members also suffered a "loss of value" of their sensitive personal information when it was stolen by hackers in the Data Breach. A robust market exists for stolen personal information. Hackers sell personal information on the dark web—an underground market for illicit activity, including the purchase of hacked personal information—at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiffs and Class Members.

76. Plaintiffs' and Class Members' stolen personal information is a valuable commodity to identity thieves. William P. Barr, former United States Attorney General, made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. One commentator confirmed, explaining that, "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud." In fact, Plaintiffs' and Class Members' personal information is currently available for purchase on the dark web and/or through private sale to other cyber criminals.

77. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiffs and Class Members gathered from underground sources, public sources, or even Plaintiffs' and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members'

information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining Social Security numbers in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

78. Plaintiffs and Class Members also suffered "benefit of the bargain" damages. Plaintiffs and Class Members overpaid for services that should have been—but were not—accompanied by adequate data security. Part of the interest and fees paid by Plaintiffs and Class Members to Nelnet were intended to be used to fund adequate data security. Plaintiffs and Class Members did not get what they paid for.

79. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming, especially because Nelnet has failed to disclose when the breach occurred or how long it lasted, forcing customers to continue to monitor their accounts indefinitely.

80. Class Members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans,

late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

81. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

82. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information (including Social Security numbers) has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

83. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches to various individuals rather than in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

VI. Nelnet's Failure to Notify Plaintiffs and Class Members in a Timely or Adequate Fashion Exacerbated the Damage

84. As detailed above, Nelnet claims to have discovered the Data Breach on July 21, 2022 yet failed to even *begin* notifying Plaintiffs and Class Members until August 26, 2022 via U.S. Mail.

85. This period of over a month could have been used by Plaintiffs and Class Members to take steps to mitigate the damage caused by the Data Breach.

86. Instead, and to protect its own financial interests, Nelnet concealed the Data Breach for over a month, allowing the unauthorized third-party to potentially exploit Plaintiffs' and Class Members' PII without any mitigation steps being taken.

87. Plaintiffs and Class Members were deprived of the opportunity to take any steps to prevent damage by Nelnet's concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members.

VII. Plaintiffs' Allegations

88. Plaintiff Bump is a citizen and resident of the Commonwealth of Massachusetts. Plaintiff Bump's student loans were assigned, without Plaintiff Bump's input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Bump was required to create a Nelnet account and provide PII to Nelnet to stay current and make payment on Plaintiff Bump's student loans. Plaintiff Bump received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Bump that Plaintiff Bump's PII was compromised in the Data Breach.

89. Plaintiff Charbonneau is a citizen and resident of the State of Illinois. Plaintiff Charbonneau's student loans were assigned, without Plaintiff Charbonneau's input or consent, to EdFinancial for servicing in 2022. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Charbonneau was required to create a Nelnet account and provide PII to Nelnet to stay current and make payment on Plaintiff Charbonneau's student loans. Plaintiff Charbonneau received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Charbonneau that Plaintiff Charbonneau's PII was compromised in the Data Breach.

90. Plaintiff Conley is a citizen and resident of the State of Arizona. Plaintiff Conley's student loans were assigned, without Plaintiff Conley's input or consent, to EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Conley was required to create a Nelnet account and provide PII to Nelnet to stay current and make payment on Plaintiff Conley's student loans. Plaintiff Conley received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Conley that Plaintiff Conley's PII was compromised in the Data Breach.

91. Plaintiff Helvey is a citizen and resident of the State of Utah. Plaintiff Helvey's student loans were assigned, without his input or consent, to EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Helvey was required to create a Nelnet account and provide PII to Nelnet to stay current and make payment on Plaintiff Helvey's student loans. Plaintiff Helvey received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Helvey that Plaintiff Helvey's PII was compromised in the Data Breach.

92. Plaintiff Iler is a citizen and resident of the State of Indiana. Plaintiff Iler's student loans were assigned, without Plaintiff Iler's input or consent, to EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Iler was required to create a Nelnet account and provide PII to Nelnet to stay current and make payments on Plaintiff Iler's student loans. Plaintiff Iler received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Iler that Plaintiff Iler's PII was compromised in the Data Breach.

93. Plaintiff Jones is a citizen and resident of the Commonwealth of Pennsylvania. Plaintiff Jones' student loans were assigned, without Plaintiff Jones' input or consent, to

EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Jones was required to create a Nelnet account and provide PII to Nelnet in order to stay current and make payments on Plaintiff Jones' student loans. Plaintiff Jones received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Jones that Plaintiff Jones' PII was compromised in the Data Breach. Since Plaintiff Jones' information was compromised in the Data Breach, two unauthorized applications for credit cards have been made in Plaintiff Jones' name, as reflected by Plaintiff Jones' credit report.

94. Plaintiff Peterson is a citizen and resident of the Commonwealth of Pennsylvania. Plaintiff Peterson's student loans were assigned, without Plaintiff Peterson's input or consent, to EdFinancial. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Peterson was required to create a Nelnet account and provide PII to Nelnet in order to stay current and make payments on Plaintiff Peterson's student loans. Plaintiff Peterson received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Peterson that Plaintiff Peterson's PII was compromised in the Data Breach.

95. Plaintiff Randall is a citizen and resident of the State of Wisconsin. Plaintiff Randall's student loans were assigned, without her input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Randall was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Randall received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Randall that Plaintiff Randall's PII was compromised in the Data Breach.

96. Plaintiff Rodriguez is a citizen and resident of the State of Michigan. Plaintiff Rodriguez's student loans were assigned, without her input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff

Rodriguez was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Rodriguez received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Rodriguez that Plaintiff Rodriguez's PII was compromised in the Data Breach.

97. Plaintiff Woods is a citizen and resident of the State of Texas. Plaintiff Woods' student loans were assigned, without her input or consent, to EdFinancial for servicing. Because EdFinancial hired Nelnet to provide online technology services, Plaintiff Woods was required to create a Nelnet account and provide PII to Nelnet. Plaintiff Woods received a letter dated August 26, 2022, via U.S. Mail with the subject "Notice of Security Incident" notifying Plaintiff Woods that Plaintiff Woods' PII was compromised in the Data Breach.

CLASS ACTION ALLEGATIONS

98. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Nationwide Class").

99. Plaintiffs reserve the right to modify, expand or amend the above Nationwide Class definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

ARIZONA SUBCLASS

100. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Arizona Subclass:

> All persons in Arizona whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Arizona Subclass").

101. Plaintiffs reserve the right to modify, expand or amend the above Arizona Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

ILLINOIS SUBCLASS

102. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Illinois Subclass:

> All persons in Illinois whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Illinois Subclass").

103. Plaintiffs reserve the right to modify, expand or amend the above Illinois Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

INDIANA SUBCLASS

104. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Indiana Subclass:

> All persons in Indiana whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Indiana Subclass").

105. Plaintiffs reserve the right to modify, expand or amend the above Indiana Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

MASSACHUSETTS SUBCLASS

106. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Massachusetts Subclass:

> All persons in Massachusetts whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Massachusetts Subclass").

107. Plaintiffs reserve the right to modify, expand or amend the above Massachusetts Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

MICHIGAN SUBCLASS

108. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Michigan Subclass:

> All persons in Michigan whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Michigan Subclass").

109. Plaintiffs reserve the right to modify, expand or amend the above Michigan Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

PENNSYLVANIA SUBCLASS

110. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Pennsylvania Subclass:

> All persons in Pennsylvania whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Pennsylvania Subclass").

111. Plaintiffs reserve the right to modify, expand or amend the above Pennsylvania Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

TEXAS SUBCLASS

112. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Texas:

> All persons in Texas whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Texas Subclass").

113. Plaintiffs reserve the right to modify, expand or amend the above Texas Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

UTAH SUBCLASS

114. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Utah Subclass:

> All persons in Utah whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Utah Subclass").

115. Plaintiffs reserve the right to modify, expand or amend the above Utah Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

WISCONSIN SUBCLASS

116. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Wisconsin Subclass:

> All persons in Wisconsin whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Wisconsin Subclass").[5]

117. Plaintiffs reserve the right to modify, expand or amend the above Wisconsin Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

118. Certification of Plaintiffs' claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can prove the elements

[5] Collectively, the Arizona Subclass, Illinois Subclass, Indiana Subclass, Massachusetts Subclass, Michigan Subclass, Pennsylvania Subclass, Texas Subclass, Utah Subclass, and Wisconsin Subclass are the "State Subclasses."

of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

119. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The Members of the Nationwide Class and the State Subclasses are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While Plaintiffs are informed and believe that there are likely millions of Members of the Classes, the precise number of Class Members is unknown to Plaintiffs. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

120. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Nelnet engaged in active misfeasance and misconduct alleged herein;

b. Whether Nelnet owed a duty to Class Members to safeguard their sensitive personal information;

c. Whether Nelnet breached its duty to Class Members to safeguard their sensitive personal information;

d. Whether Nelnet knew or should have known that its data security systems and monitoring processes were deficient;

e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of the Data Breach;

f. Whether Nelnet's failure to provide adequate security proximately caused Plaintiffs' and Class Members' injuries; and

g. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

121. **Typicality.** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of all Class and Subclass Members because Plaintiffs, like other Class and Subclass Members, suffered theft of their sensitive personal information in the Data Breach.

122. **Adequacy of Representation.** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are Members of the Classes and State Subclasses and their interests do not conflict with the interests of other Class and Subclass Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intends to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

123. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered

in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Nelnet, so it would be impracticable for Members of the Class to individually seek redress for Nelnet's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

124. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Nelnet has acted, or refused to act, on grounds generally applicable to the Nationwide Class and California Subclass such that final declaratory or injunctive relief is appropriate.

125. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on newly learned facts or legal developments that arise following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

126. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

127. Nelnet obtained Plaintiffs' and Class Members' sensitive personal information in connection with Plaintiffs and Class Members signing up for Nelnet's wireless services.

128. By collecting and maintaining sensitive personal information, Nelnet had a common law duty of care to use reasonable means to secure and safeguard the sensitive personal information and to prevent disclosure of the information to unauthorized individuals. Nelnet's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

129. Nelnet owed a duty of care to Plaintiffs and Class Members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

130. Nelnet's duty of care arose as a result of, among other things, the special relationship that existed between Nelnet and its customers. Nelnet was the only party in a position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur that would result in substantial harm to consumers.

131. Nelnet was subject to an "independent duty" untethered to any contract between Plaintiffs and Class Members and Nelnet.

132. 91. Nelnet breached its duties, and thus was negligent, by failing to use reasonable measures to protect customers' sensitive personal information. Nelnet's negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees to protect against malware;

b. failure to comply with industry standards for software and server security;

c. failure to track and monitor access to its network and personal information;

d. failure to limit access to those with a valid purpose;

e. failure to adequately staff and fund its data security operation;

f. failure to remove, delete, or destroy highly sensitive personal information of consumers that is no longer being used for any valid business purpose;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing personal information from its network while the Data Breach was taking place.

133. It was foreseeable to Nelnet that a failure to use reasonable measures to protect its customers' sensitive personal information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Nelnet given the known frequency of data breaches and various warnings from industry experts.

134. As a direct and proximate result of Nelnet's negligence, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

135. Plaintiffs and Class Members are also entitled to injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

136. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

138. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Nelnet's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

139. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

140. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

141. As a direct and proximate result of Nelnet's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

142. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

143. Plaintiffs and Class Members are also entitled to injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

144. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

145. When Plaintiffs and Class Members provided their sensitive personal information to Nelnet in exchange for Nelnet's services, they entered into implied contracts with Nelnet under which Nelnet agreed to take reasonable steps to protect their sensitive personal information.

146. Nelnet solicited and invited Plaintiffs and Class Members to provide their sensitive personal information as part of Nelnet's regular business practices. Indeed, to sign up for a Nelnet account—which is required to make payments online to loan serviced by companies that hire Nelnet for web portal and payment processing services—Nelnet requires customers to provide sensitive personal information including Social Security numbers, to obtain Nelnet's services. Plaintiffs and Class Members accepted Nelnet's offers and provided their sensitive personal information Nelnet.

147. Plaintiffs and Class Members reasonably believed and expected that Nelnet's data security practices complied with relevant laws, regulations, and industry standards when they entered into the implied contracts with Nelnet.

148. Plaintiffs and Class Members paid money to Nelnet and Plaintiffs and Class Members therefore reasonably believed and expected that Nelnet would use part of those funds to obtain adequate data security. Nelnet failed to do so.

149. Plaintiffs and Class Members would not have provided their sensitive personal information to Nelnet in the absence of Nelnet's implied promise to keep their sensitive personal information reasonably secure.

150. Plaintiffs and Class Members fully performed their obligations under the implied contracts by paying money to Nelnet.

151. Nelnet breached its implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures.

152. As a direct and proximate result of Nelnet's breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

153. Plaintiffs and Class Members are also entitled to injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

154. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

155. Plaintiffs and Class Members conferred a monetary benefit upon Nelnet in the form of monies paid while utilizing Nelnet's online services.

156. Nelnet appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Nelnet also benefited from the receipt of Plaintiffs' and Class Members' sensitive personal information as this was utilized by Nelnet to send bills and process payments for services, among other things.

157. The monies Plaintiffs and Class Members paid to Nelnet were supposed to be used by Nelnet, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

158. Nelnet's conduct caused Plaintiffs and Class Members to suffer actual damages in an amount equal to the difference in value between what they paid for (Nelnet's services made with adequate data privacy and security practices and procedures), and what they actually received (Nelnet's services without adequate data privacy and security practices and procedures).

159. In equity and good conscience, Nelnet should not be permitted to retain the money belonging to Plaintiffs and Class Members because Nelnet failed to implement, or adequately implement, the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

160. Nelnet should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF CONFIDENCE
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

161. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

162. Plaintiffs and Class Members maintained a confidential relationship with Nelnet whereby Nelnet undertook a duty not to disclose to unauthorized parties the PII provided by Plaintiffs and Class Members to Nelnet to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

163. Nelnet knew Plaintiffs' and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

164. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Nelnet failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

165. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

166. But for Nelnet's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Nelnet's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

167. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Nelnet's unauthorized disclosure of Plaintiffs' and Class Members' PII. Nelnet knew its computer systems and technologies for accepting, securing, and storing

COUNT VI
INVASION OF PRIVACY – INSTUSION UPON SECLUSION
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

168. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

169. Plaintiffs shared PII with Nelnet that Plaintiffs wanted to remain private and non-public.

170. Plaintiffs reasonably expected that the PII they shared with Nelnet would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

171. Nelnet intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

172. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Nelnet unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

173. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other PII.

174. Nelnet's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

175. As a direct and proximate result of Nelnet's invasions of privacy, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Nelnet; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Nelnet's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT VII
ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521, *et seq.*

176. Plaintiff Conley individually and on behalf of the Arizona Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

177. Nelnet is a "person" as defined by A.R.S. § 44-1521(6).

178. Nelnet advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

179. Nelnet engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A).

180. Nelnet's unfair and deceptive acts and practices included:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Conley's and Arizona Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Conley's and Arizona Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Conley's and Arizona Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Conley's and Arizona Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Conley's and Arizona Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Conley's and Arizona Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

181. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

182. Nelnet intended to mislead Plaintiffs and Arizona Subclass Members and induce them to rely on its misrepresentations and omissions.

183. Had Nelnet disclosed to Plaintiff Conley and Arizona Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions

of consumers, including Plaintiff Conley and the Arizona Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Conley and the Arizona Subclass Members acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

184. Nelnet acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff Conley's and Arizona Subclass Members' rights.

185. As a direct and proximate result of Nelnet's unfair and deceptive acts and practices, Plaintiff Conley and Arizona Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

186. Plaintiff Conley and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VIII
ILLINOIS PERSONAL INFORMATION PROTECTION ACT,
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*
(On behalf of the Plaintiff Charbonneau and the Illinois Subclass)

187. Plaintiff Charbonneau, individually and on behalf of the Illinois Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

188. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), Nelnet is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

189. Plaintiff Charbonneau's and Illinois Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under 815 Ill. Comp. Stat. § 530/5.

190. As a Data Collector, Nelnet is required to notify Plaintiff Charbonneau and Illinois Subclass Members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

191. By failing to disclose the Nelnet data breach in the most expedient time possible and without unreasonable delay, Nelnet violated 815 Ill. Comp. Stat. § 530/10(a).

192. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

193. As a direct and proximate result of Nelnet's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff Charbonneau and Illinois Subclass Members suffered damages, as described above.

194. Plaintiff Charbonneau and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Nelnet's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT IX
ILLINOIS CONSUMER FRAUD ACT,
815 Ill. Comp. Stat. §§ 505, et seq.

195. Plaintiff Charbonneau, individually and on behalf of the Illinois Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

196. Nelnet is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

197. Plaintiff Charbonneau and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

198. Nelnet's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

199. Nelnet's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Charbonneau's and Illinois Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade

Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Charbonneau's and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Charbonneau's and Illinois Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

200. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

201. Nelnet intended to mislead Plaintiff Charbonneau and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

202. The above unfair and deceptive practices and acts by Nelnet were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

203. Nelnet acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff Charbonneau's and Illinois Subclass Members' rights.

204. As a direct and proximate result of Nelnet's unfair, unlawful, and deceptive acts and practices, Plaintiff Charbonneau and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

205. Plaintiff Charbonneau and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT X
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,
815 Ill. Comp. Stat. §§ 510/2, *et seq.*

206. Plaintiff Charbonneau, individually and on behalf of the Illinois Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

207. Nelnet is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

208. Nelnet engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

209. Nelnet's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Charbonneau's and Illinois Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Charbonneau's and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Charbonneau's and Illinois Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois

laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

210. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

211. The above unfair and deceptive practices and acts by Nelnet were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Charbonneau and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

212. As a direct and proximate result of Nelnet's unfair, unlawful, and deceptive trade practices, Plaintiff Charbonneau and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

213. Plaintiff Charbonneau and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT XI
INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code §§ 24-5-0.5-1, *et seq.*
(On behalf of Plaintiff Iler and the Indiana Subclass)

214. Plaintiff Iler individually and on behalf of the Indiana Subclass, repeats and realleges all allegations as if fully set forth herein.

215. Nelnet is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

216. Nelnet is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

217. Nelnet engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

218. Nelnet's representations and omissions include both implicit and explicit representations, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Iler's and Indiana Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Iler's and Indiana Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Iler's and Indiana Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Iler's and Indiana Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Iler's and Indiana Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Iler's and Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

219. Nelnet's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

220. The injury to consumers from Nelnet's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

221. Consumers could not have reasonably avoided injury because Nelnet's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the

inadequacy of its data security, Nelnet created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

222. Nelnet's inadequate data security had no countervailing benefit to consumers or to competition.

223. Nelnet's acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Nelnet's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Nelnet's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Nelnet concerning the state of Nelnet security, and because it is functionally impossible for consumers to obtain credit without their PII being in Nelnet's systems.

d. Because Nelnet took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

224. Nelnet also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

225. Nelnet intended to mislead Plaintiff Iler and Indiana Subclass Members and induce them to rely on its misrepresentations and omissions.

226. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

227. Had Nelnet disclosed to Plaintiff Iler and Indiana Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Iler and the Indiana Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Iler and Indiana Subclass Members acted

reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

228. Nelnet had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Nelnet and Plaintiff Iler and the Indiana Subclass as described herein. In addition, such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff Iler and the Indiana Subclass-and Nelnet, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Nelnet. Nelnet's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff Iler and the Indiana Subclass that contradicted these representations.

229. Nelnet acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff Iler's and Indiana Subclass Members' rights. Nelnet's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

230. Nelnet's conduct includes incurable deceptive acts that Nelnet engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-

2(a)(8). As a direct and proximate result of Nelnet's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff Iler and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

231. Nelnet's violations present a continuing risk to Plaintiff Iler and Indiana Subclass Members as well as to the public.

232. Plaintiff Iler and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

COUNT XII
MASSACHUSETTS CONSUMER PROTECTION ACT,
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.*
(On behalf of Plaintiff Bump and the Massachusetts Subclass)

233. Plaintiff Bump, individually and on behalf of the Massachusetts Subclass, repeats and realleges all allegations as if fully set forth herein.

234. Nelnet and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

235. Nelnet operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

236. Nelnet advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

237. Nelnet engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Bump's and Massachusetts Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bump's and Massachusetts Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Bump's and Massachusetts Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bump's and Massachusetts Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Bump's and Massachusetts Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bump's and Massachusetts Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the

Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

238. Nelnet's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Nelnet solely held the true facts about its inadequate security for PII, which Plaintiff Bump and the Massachusetts Subclass could not independently discover.

239. Consumers could not have reasonably avoided injury because Nelnet's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Nelnet created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

240. Nelnet's inadequate data security had no countervailing benefit to consumers or to competition.

241. Nelnet intended to mislead Plaintiff Bump and the Massachusetts Subclass and induce them to rely on its misrepresentations and omissions. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

242. Nelnet acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff Bump's and Massachusetts Subclass Members' rights.

243. As a direct and proximate result of Nelnet's unfair and deceptive, Plaintiff Bump and the Massachusetts Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein,

including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

244. Plaintiff Bump and the Massachusetts Subclass seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XIII
MICHIGAN IDENTITY THEFT PROTECTION ACT,
Mich. Comp. Laws Ann. §§ 445.72, *et seq*
(On behalf of Plaintiff Rodriguez and the Michigan Subclass)

245. Plaintiff Rodriguez individually, and on behalf of the Michigan Subclass, repeats and realleges all allegations as if fully set forth herein.

246. Nelnet is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

247. Plaintiff Rodriguez's and Michigan Subclass Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

248. Nelnet is required to accurately notify Plaintiff Rodriguez and Michigan Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

249. Because Nelnet discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons),

Nelnet had an obligation to disclose the Nelnet data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

250. By failing to disclose the Nelnet data breach in a timely and accurate manner, Nelnet violated Mich. Comp. Laws Ann. § 445.72(4).

251. As a direct and proximate result of Nelnet's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff Rodriguez and Michigan Subclass Members suffered damages, as described above.

252. Plaintiff Rodriguez and Michigan Subclass Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT XIV
MICHIGAN CONSUMER PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.903, *et seq.*

253. Plaintiff Rodriguez individually, and on behalf of the Michigan Subclass, repeats and realleges all allegations as if fully set forth herein.

254. Nelnet and Michigan Subclass Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

255. Nelnet advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

256. Nelnet engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.

257. Nelnet's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Rodriguez's and Michigan Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rodriguez and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Rodriguez's and Michigan Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rodriguez's and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Rodriguez's and Michigan Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rodriguez's and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

258. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

259. Nelnet intended to mislead Plaintiff Rodriguez and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

260. Nelnet acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff Rodriguez and Michigan Subclass Members' rights.

261. As a direct and proximate result of Nelnet's unfair, unconscionable, and deceptive practices, Plaintiff Rodriguez and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

262. Plaintiff Rodriguez and the Michigan Subclass seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

COUNT XV
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*
(On behalf of Plaintiff Peterson, Plaintiff Jones, and the Pennsylvania Subclass)

263. Plaintiff Peterson and Plaintiff Jones individually, and on behalf of the Pennsylvania Subclass, repeat and reallege all allegations as if fully set forth herein.

264. Nelnet is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

265. Plaintiff Peterson, Plaintiff Jones, and the Pennsylvania Subclass purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

266. Nelnet engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

267. Nelnet's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members'

PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

268. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

269. Nelnet intended to mislead Plaintiff Peterson, Plaintiff Jones, and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

270. Had Nelnet disclosed to Plaintiff Peterson, Plaintiff Jones, and the Pennsylvania Subclass that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII

regarding millions of consumers, including Plaintiff Peterson, Plaintiff Jones, and the Pennsylvania Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Peterson, Plaintiff Jones, and the Pennsylvania Subclass acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

271. Nelnet acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff Peterson's, Plaintiff Jones', and Pennsylvania Subclass Members' rights.

272. As a direct and proximate result of Nelnet's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff Peterson's, Plaintiff Jones', and the Pennsylvania Subclass' reliance on them, Plaintiff Peterson, Plaintiff Jones, and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

273. Plaintiff Peterson, Plaintiff Jones, and the Pennsylvania Subclass seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT XVI
DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT,
Texas Bus. & Com. Code §§ 17.41, et seq.
(On behalf of Plaintiff Woods and the Texas Subclass)

274. Plaintiff Woods individually, and on behalf of the Texas Subclass, repeats and realleges all allegations if fully set forth herein.

275. Nelnet is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

276. Plaintiff Woods and Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

277. Nelnet advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

278. Nelnet engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

279. Nelnet's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Woods' and Texas Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Woods' and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Woods' and Texas Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Woods' and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Woods' and Texas Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Woods' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

280. Nelnet intended to mislead Plaintiff Woods and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

281. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

282. Had Nelnet disclosed to Plaintiff Woods and Texas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Woods and the Texas Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Woods and Texas Subclass Members acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

283. Nelnet had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff Woods and the Texas Subclass, and Nelnet because consumers are unable to

fully protect their interests regarding their data, and placed trust and confidence in Nelnet. Nelnet's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

284. Nelnet engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Nelnet engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

285. Consumers, including Plaintiff Woods and Texas Subclass Members, lacked knowledge about deficiencies in Nelnet's data security because this information was known exclusively by Nelnet. Consumers also lacked the ability, experience, or capacity to secure the PII in Nelnet's possession or to fully protect their interests regarding their data. Plaintiff Woods and Texas Subclass Members lack expertise in information security matters and do not have access to Nelnet's systems to evaluate its security controls. Nelnet took advantage of its special skill and access to PII to hide its inability to protect the security and confidentiality of Plaintiff Woods' and Texas Subclass Members' PII.

286. Nelnet intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that

would result. The unfairness resulting from Nelnet's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Nelnet data breach, which resulted from Nelnet's unconscionable business acts and practices, exposed Plaintiff Woods and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

287. Nelnet acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff Woods' and Texas Subclass Members' rights.

288. As a direct and proximate result of Nelnet's unconscionable and deceptive acts or practices, Plaintiff Woods and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach. Nelnet's unconscionable and deceptive acts or practices were a producing cause of Plaintiff Woods' and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

289. Nelnet's violations present a continuing risk to Plaintiff Woods and Texas Subclass Members as well as to the public.

290. Plaintiff Woods and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

COUNT XVII
UTAH CONSUMER SALES PRACTICES ACT,
Utah Code §§ 13-11-1, et seq.
(On behalf of Plaintiff Helvey and the Utah Subclass)

291. Plaintiff Helvey individually, and on behalf of the Utah Subclass, repeats and realleges all allegations if fully set forth herein.

292. Nelnet is a "person," as defined by Utah Code § 13-11-1(5).

293. Nelnet is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

294. Nelnet engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Helvey's and Utah Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Helvey's and Utah Subclass Members'

PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;

d. d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Helvey's and Utah Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Helvey's and Utah and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Helvey's and Utah Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Helvey's and Utah Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201.

295. Nelnet intended to mislead Plaintiff Helvey and Utah Subclass Members and induce them to rely on its misrepresentations and omissions.

296. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

297. Had Nelnet disclosed to Plaintiff Helvey and Utah Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Nelnet would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Nelnet was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Helvey and the Utah Subclass. Nelnet accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Helvey and the Utah Subclass Members acted reasonably in relying on Nelnet's misrepresentations and omissions, the truth of which they could not have discovered.

298. Nelnet had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff Helvey and the Utah Subclass, and Nelnet because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Nelnet. Nelnet's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff Helvey and the Utah Subclass that contradicted these representations.

299. Nelnet intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

a. Indicating that the subject of a consumer transaction has approval, performance characteristics, accessories, uses, or benefits, if it has not;

b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;

c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not; and

d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (*e.g.* more data security) than the supplier intends.

300. Nelnet engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Nelnet's acts and practices unjustly imposed hardship on Plaintiff Helvey and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their PII. The deficiencies in Nelnet's data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff Helvey and the Utah Subclass when the Data Breach occurred.

301. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required Nelnet to adequately secure PII in its possession. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff Helvey and the Utah Subclass and Nelnet, which has control over the PII in its

possession. Industry standards-including those reflected in the security requirements of the FTC and dictate that Nelnet adequately secure the PII in its possession.

302. As a direct and proximate result of Nelnet's unconscionable and deceptive acts or practices, Plaintiff Helvey and Utah Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

303. Nelnet's violations present a continuing risk to Plaintiff Helvey and Utah Subclass Members as well as to the public.

304. Plaintiff Helvey and Utah Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, et seq.; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VIII
NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION, Wis. Stat. §§ 134.98(2), *et seq.*

305. Plaintiff Randall individually, and on behalf of the Utah Subclass, repeats and realleges all allegations if fully set forth herein.

306. Nelnet is a business that maintains or licenses personal information (for the purpose of this count, "PII"), as defined by Wis. Stat. § 134.98(2).

307. Plaintiff Randall's and Wisconsin Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Wis. Stat. § 134.98(1)(b).

308. Nelnet is required to accurately notify Plaintiff Randall and Wisconsin Subclass Members if it knows that PII in its possession has been acquired by a person whom it has not authorized to acquire the PII within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

309. Because Nelnet knew that PII in its possession had been acquired by a person whom it has not authorized to acquire the PII, Nelnet had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

310. By failing to disclose the Nelnet data breach in a timely and accurate manner, Nelnet violated Wis. Stat. § 134.98(2).

311. As a direct and proximate result of Nelnet's violations of Wis. Stat. § 134.98(3)(a), Plaintiff Randall and Wisconsin Subclass Members suffered damages, as described above.

312. Plaintiff Randall and Wisconsin Subclass Members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT XIX
WISCONSIN DECEPTIVE TRADE PRACTICES ACT, Wis. Stat. § 100.18

313. Plaintiff Randall individually, and on behalf of the Utah Subclass, repeats and realleges all allegations if fully set forth herein.

314. Nelnet is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

315. Plaintiff Randall and Wisconsin Subclass Members are members of "the public," as defined by Wis. Stat. § 100.18(1).

316. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Nelnet to members of the public for sale, use, or distribution, Nelnet made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

317. Nelnet also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

318. Nelnet's deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Randall's and Wisconsin Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Randall's and Wisconsin Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Randall's and Wisconsin Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Randall's and Wisconsin Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Randall's and Wisconsin Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Randall's and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

319. Nelnet intended to mislead Plaintiff Randall and Wisconsin Subclass Members and induce them to rely on its misrepresentations and omissions.

320. Nelnet's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Nelnet's data security and ability to protect the confidentiality of consumers' PII.

321. Nelnet had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Wisconsin Subclass-and Nelnet, because

consumers are unable to fully protect their interests about their data and placed trust and confidence in Nelnet. Nelnet's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

322. Nelnet's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

323. Nelnet acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Randall's and Wisconsin Subclass Members' rights.

324. As a direct and proximate result of Nelnet's deceptive acts or practices, Plaintiff Randall and Wisconsin Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Nelnet's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

325. Nelnet had an ongoing duty to all Nelnet customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

326. Plaintiff Randall and Wisconsin Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

COUNT XX
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of the Nationwide Class, or alternatively, the State Subclasses)

327. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

328. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

329. An actual controversy has arisen in the wake of the Data Breach regarding Nelnet's present and prospective common law and statutory duties to reasonably safeguard its customers' sensitive personal information and whether Nelnet is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches. Plaintiffs alleges that Nelnet's data security practices remain inadequate.

330. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

331. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Nelnet continues to owe a legal duty to secure consumers'

sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

332. The Court also should issue corresponding prospective injunctive relief requiring Nelnet to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

333. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach at Nelnet occurs, Plaintiffs and Class Members will not have an adequate remedy at law, because not all of the resulting injuries are readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

334. The hardship to Plaintiffs and Class Members if an injunction does not issue greatly exceeds the hardship to Nelnet if an injunction is issued. If another data breach occurs at Nelnet, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Nelnet of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Nelnet has a pre-existing legal obligation to employ such measures.

335. Issuance of the requested injunction will serve the public interest by preventing another data breach at Nelnet, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

336. Plaintiffs, on behalf of all others similarly situated, request that the Court enter judgment against Nelnet including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiffs as representative of the applicable Classes and appointing Plaintiffs' counsel as Class counsel;

C. An award to Plaintiffs and the Classes of compensatory, consequential, statutory, restitutionary, and treble damages as set forth above;

D. Ordering injunctive relief requiring Nelnet to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members; (iv) timely notify consumers of any future data breaches; and (v) delete or destroy any legacy consumer data that it is not necessary to keep for business purposes;

E. Entering a declaratory judgment stating that Nelnet owes a legal duty to secure consumers' sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

337. Plaintiffs demands a trial by jury for all issues so triable.

DATED this 14th day of September, 2022.

PAMELA BUMP, MELISSA CHARBONNEAU, DOUGLAS CONLEY, NOAH HELVEY, DALLIN ILER, DUSTIN JONES, DEVINNE PETERSON, JUSTIN RANDALL, SOFIA RODRIGUEZ, and RACHEL WOODS, individually and on behalf of all others similarly situated, Plaintiffs

/s/ Joel M. Carney

Joel M. Carney, #21922
Jeana L. Goosmann, #22545
Joseph V. Messineo, #21981
GOOSMANN LAW FIRM, PLC
17838 Burke Street, Ste. 250
Omaha, NE 68118
Telephone: (402) 280-7648
carneyj@goosmannlaw.com
goosmannj@goosmannlaw.com
messineoj@goosmannlaw.com

and

Steven L. Bloch (*pro hac vice* forthcoming)
Ian W. Sloss (*pro hac vice* forthcoming)
Zachary Rynar (*pro hac vice* forthcoming)
SILVER GOLUB & TEITELL LLP
One Landmark Square
Fifteenth Floor
Stamford, Connecticut 06901
Telephone: (203) 325-4491
Fax: (203) 325-3769
sbloch@sgtlaw.com
isloss@sgtlaw.com
zrynar@sgtlaw.com

Christian Levis (*pro hac vice* forthcoming)
Johnathan Seredynski (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
jseredynski@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com